**Answers and grading comments for Assignment 6 – Week 7**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**

**(1) What is the password that you use to log on to the Infosys system? I ask because I need to log on as you to verify that you are seeing your assignment/lab grades correctly. Thanks for your understanding.**  
 **ANS:**  
  
With all due respect Professor, that is none of your business.

**(2) Which of the following passwords are susceptible to a dictionary attack?**

a) Maharishi  
b) flobbydr0mMel  
c) ice cream  
d) fjkakjkjvadoifj;lajd;lkjdfjkioopaj;ajkiojgadlkjao;ijpiojol;jkl;ajo;dfpoije  
e) DPOTMPSIA (first letters of the sentence Daily Practice Of Transcendental Meditation Promotes Skill In Action)

**ANS: a,c**

Dictionary attacks work on passwords that are derived from words in a dictionary. They are not brute force attacks which try all possible passwords. It is unlikely that 2nd, 4th and 5th passwords could be derived from any word in a dictionary.

**(3) The ©Drib system required that users first login to a regular account before logging into a sysadmin (superuser) account.  Suppose that when the sysadmin login procedure asks for the password, it cannot open the password file (perhaps it’s been corrupted or there is some other problem with the file).  Suppose that when this extremely unusual and unlikely situation occurs, the login procedure allows the user access to the sysadmin account so he/she can fix the problem.  Which principles are being violated by this mechanism?  Which principles are being met?**

**ANS:**

Violated: Complete mediation  
Met: Psychological acceptibility

**(4) Which of the following can be used to establish the identity of an external entity (a user of the computer system)?**

a) Where the entity is  
b) What the entity knows  
c) What the entity has  
d) The age of the entity  
e) What the entity is  
f)  When the entity logged on

**ANS: a, b, c, e**

See section 11.1 of the textbook.

**(5) After reading all the literature on passwords, these appear to be the recommendations:**

  **1. The password should be resistant to a dictionary attack  
  2. The password should be changed regularly  
  3. The password should not be written down  
  4. Different passwords should be used on different accounts**

**What principle do these recommendations violate?**

a) Principle of least privilege  
b) Principle of fail-safe defaults  
c) Principle of economy of mechanism  
d) Principle of complete mediation  
e) Principle of open design  
f) Principle of separation of privilege  
g) Principle of least common mechanism  
h) Principle of psychological acceptibility  
  
**ANS: h**  
  
It is unreasonable for a human being with a typical human brain (which is used for all sorts of things) to be able to do all of these things comfortably. This is a classic violation of the principle of psychological acceptibility. There is a lot of research now how to make a system both secure and reasonably easy to use. The equation S=1/C where S=security and C=convenience demonstrates the problem. The more convenient a system is (e.g., no passwords required), the more insecure it is. And the less convenient it is (e.g., 14 character strong passwords required, with periodic surprise inspections of your office looking for written-down passwords), the more secure it is. Security and Convenience have to be integrated; an important principle of SCI is the integration of opposites.  
Several students chose "separation of privilege" picking up on fact that using different passwords for different systems is a kind of separation of privilege. But the question asked which principle was **violated**.  
Several students chose "economy of mechanism" because of the complexity. Economy of mechanism means that the code of programs is simple, the simpler the code, the fewer bugs are likely to be in it. The complexity we are talking about here is psychological.  
Most students who made some clarification of a wrong answer got partial credit. Unfortunately, it is usually the case that the clarifications are done by students who got the answer right!

**(6) A password is information associated with an external entity that confirms the identity of that entity.  What security measures should be taken to ensure the correctness of this binding?  Give 3 internal measures by the login program and 3 external measures by the user.**

**ANS:**

Internal

1. Use SSL  
2. Look up login name and password in database.  
3. Don’t let the login error reveal whether login or password is bad.

External

1. Password is hard to guess  
2. Different passwords on different systems  
3. Don't write password down

**(7) Your labs are saved in a database that is password protected. Imagine that you were maintaining the CS466 web site and you had to choose a password for the database. Give an example of a password that you might choose. Keep in mind that the password is primarily used by the web application to store and retrieve data from the database. Manual interaction with the database, such as typing in SQL queries in SQL Management Studio or/and IDE for MySQL, is kept to a minimum.**

**ANS:**

I was looking for a really ugly string of characters. It was not really important that it had to be easy to memorize since the password was stored in a configuration file that was used by the web application. You lost points if your password was too logical, e.g., **MUM\_cs466\_May2012**. Somebody with a good intuitive sense (a meditator?) might have a chance of guessing it.

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**